GUIDEBOOK

CISO Guide to Malware and Ransomware

Transforming Unseen Risks Into Measurable Resilience

Abnormal

Table of Contents

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

The Current State of Malware and Ransomware

For decades, malware has played a central role in cyberattacks—stealing data, disrupting operations, and compromising systems. But today, it looks very different. Enabled by generative AI, modern malware is adaptive, contextually aware, and skilled at concealing itself within our most trusted environments.

68%

Share of malware attacks that occurred via email in 2024

Statista

$5.8M

Average total cost of ransomware attacks in 2025

IBM Cost of a Data Breach Report 2025

37%

Increase in ransomware incidents since 2024

Verizon 2025 Data Breach Investigations Report

Rising Frequency and Complexity

According to the **Verizon 2025 Data Breach Investigations Report**, ransomware attacks have increased by 37% since 2024. This surge reflects not only higher attack volumes but also the growing sophistication of threat actors who are increasingly leveraging artificial intelligence to enhance their operations. AI is being used to automate reconnaissance, craft more convincing phishing lures, and rapidly generate new malware variants designed to evade traditional detection methods. Even when one strain is blocked, hundreds of AI-generated mutations are ready to take its place—each slightly altered to bypass signature-based defenses.

Modern malware is no longer limited to basic trojans or static ransomware payloads. Instead, we see fileless malware that runs entirely in memory, advanced loaders that install persistence mechanisms, and multi-stage campaigns that span email, SaaS applications, and cloud storage. These techniques allow attackers to bypass traditional defenses such as secure email gateways and sandboxing solutions, which often depend on signatures or static indicators. However, email remains the primary entry point for malware, accounting for **68% of all attacks in 2024**.

Ransomware in particular has evolved from a nuisance attack to one of the most financially devastating forms of cybercrime, with a total cost averaging $5.8 million, according to IBM's 2025 **Cost of a Data Breach Report**. And now, generative AI has taken this evolution even further. By automating realistic phishing lures, adaptive malware, and polymorphic code, it gives attackers the power to scale campaigns at machine speed—making today's threats not just more frequent and complex, but faster, smarter, and harder to stop.

For CISOs, these rapidly advancing threats signal the breaking point for legacy tools and the necessity of AI-powered security.

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Types of Malware

As malware continues to grow in frequency, speed, and complexity, it has also diversified in form. What was once a relatively uniform threat, limited to self-replicating viruses or standalone ransomware, has evolved into a dynamic ecosystem of attack types and delivery methods.

Each variant is designed to exploit not only technical vulnerabilities but also the people and processes that make up modern organizations.

Attachment-Based Malware

Email attachments remain one of the most common vehicles for malware delivery. Attackers embed malicious code in files that appear legitimate, such as invoices, shipping confirmations, or HR documents, and rely on users' trust to open them. Common attachment types include PDFs, Microsoft Word or Excel files with malicious macros, compressed ZIP archives, and executable files disguised as benign content.

Once opened, the file typically triggers a download of additional malware, installs a trojan, or exploits a known software vulnerability. Even sophisticated detection systems can miss these threats when the payload is encrypted, password-protected, or otherwise concealed.

Key Risks:

- Direct system compromise and credential theft
- Delivery of ransomware or remote access trojans (RATs)
- Exploitation of zero-day vulnerabilities in document readers

Link-Based Malware

Malware delivered through hyperlinks is another prevalent vector. Instead of attaching a file, attackers send URLs that lead to malicious websites, credential-harvesting portals, or file downloads. Links often appear within legitimate-looking messages from vendors, cloud storage services, or internal systems.

To bypass defenses, attackers may use redirection chains, link shorteners, or compromised legitimate domains. Some campaigns employ "time-delayed activation," modifying the destination URL after delivery to evade scanning tools.

Key Risks:

- Credential harvesting through phishing or fake login pages
- Drive-by downloads that automatically install malware
- Exploitation of cloud storage or document-sharing tools

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Payloadless (Fileless) Attacks

Payloadless or fileless malware represents a newer and more insidious threat class. These campaigns rely on legitimate system tools and trusted processes to execute malicious commands directly in memory. Attackers often exploit PowerShell, WMI, or other built-in administrative utilities to perform their objectives without ever writing files to disk.

Because no file artifacts are left behind, these attacks are notoriously difficult to detect using conventional antivirus or signature-based systems. Many payloadless attacks are paired with social engineering, convincing a user to perform an action that grants access, executes a command, or authorizes a transfer.

Key Risks:

- Data exfiltration and lateral movement within the network
- Credential harvesting through legitimate processes
- Persistent access achieved through registry or script modification

Ransomware

Ransomware is among the most financially damaging and publicly visible forms of malware. It encrypts data and demands payment, usually in cryptocurrency, in exchange for a decryption key. Many modern ransomware groups now employ double extortion tactics, threatening to leak stolen data if the ransom is not paid.

Ransomware often begins as a phishing email, malicious attachment, or credential compromise that allows lateral movement and privilege escalation inside the network. Once deployed, it can spread rapidly across systems, encrypting files and disabling backups.

And the impact is growing. According to data from **Cybersecurity Ventures**, ransomware losses are predicted to exceed a staggering $275 billion per year in 2031.

Key Risks:

- Loss of access to critical systems and operational disruption
- Permanent data loss or public data exposure
- Financial and reputational damage

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Why the Ransomware Threat Is Increasing

Ransomware has always been profitable, but the tactics and tools available to operators today have amplified its reach and impact. Threat actors are evolving at machine speed, taking cues from nation-state techniques and adapting them for financial gain. The result is a wave of campaigns that are more creative, more destructive, and more difficult to defend against than ever before.

One of the most significant shifts is the move beyond simple file encryption. Modern operators employ double and even triple extortion, where stolen data is used as additional leverage. Victims not only face locked systems but also the threat of public exposure or regulatory fines if sensitive information is leaked.

At the same time, attackers are weaponizing new technologies to make entry points nearly indistinguishable from legitimate communication. AI-powered phishing uses generative models to craft lures that mimic human tone and context with startling accuracy, erasing many of the red flags employees once relied on to identify scams. Quishing, or QR code–based phishing, bypasses traditional link scanners entirely, directing users to malicious sites under the guise of convenience.

These techniques are no longer confined to a single vector. Increasingly, adversaries are leveraging cross-channel payload delivery, blending email, SaaS applications, and cloud file-sharing platforms to spread ransomware while avoiding detection. By moving fluidly across trusted channels, attackers exploit the interconnected nature of today's enterprise environments.

Perhaps the most concerning trend is the rise of ransomware-as-a-service (RaaS). In this model, sophisticated operators build and maintain ransomware platforms, then license them to affiliates who conduct the actual attacks. These kits come complete with infrastructure, payment portals, and even customer "support." The result is a professionalized cybercrime economy where technical expertise is no longer a barrier to entry. Even low-skill actors can launch enterprise-scale campaigns, dramatically expanding the pool of adversaries targeting organizations worldwide.

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Impact and Risks to the Modern Business

The rise of modern malware and ransomware has turned cybersecurity into a central business issue. Attacks no longer just disable systems. They disrupt operations, drain financial resources, damage reputation, and erode trust across every level of the organization. Understanding the full scope of these impacts helps leaders make informed decisions about where to invest and how to build resilience.

Direct Costs

The most visible impact of a malware or ransomware incident comes from direct financial loss. These costs include ransom payments, system recovery, data restoration, and the deployment of forensic and response teams. According to the FBI's **2024 IC3 Annual Report**, ransomware costs totaled $106.4 million since 2022, though large enterprises often face significantly higher expenses when critical systems are affected.

Direct costs can escalate quickly. Beyond the ransom itself, organizations may need to rebuild infrastructure, pay for regulatory fines, or manage contractual penalties related to service disruptions. For industries bound by data protection laws—such as healthcare, finance, or public services—the financial consequences can be compounded by compliance violations and mandatory breach notifications.

Indirect Costs

The secondary effects of malware incidents often outweigh the immediate damage. Prolonged downtime disrupts normal operations and prevents revenue generation, while customers and partners may lose confidence in the organization's ability to protect their data. Research shows that **35% of companies** affected by ransomware experience lasting reputational damage long after systems are restored.

Employee productivity and morale are also affected. IT and security teams shift focus from innovation to containment, delaying other strategic initiatives. For publicly traded companies, cyber incidents can lead to stock volatility, with share prices declining following public disclosure. Insurance premiums, compliance costs, and internal audit requirements may increase for years after an incident.

Scale of Damage

Modern malware rarely stops at a single point of failure. Once inside, attackers often move laterally through connected systems—compromising multiple departments, subsidiaries, or even third-party partners. A single infected endpoint or stolen credential can cascade through shared applications and networks, affecting thousands of users and critical services.

The widespread use of cloud-based collaboration and remote access tools has expanded these risks. Attackers exploit the interconnectivity of modern IT environments to amplify their reach, turning one compromise into many.

These ripple effects highlight the fact that malware incidents are no longer isolated technical problems; they are enterprise-wide crises. Effective recovery requires coordination between cybersecurity, operations, legal, communications, and executive leadership. In the modern business environment, the impact of malware extends far beyond IT, striking at the core of business continuity and trust.

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Why Malware Is Successful

Despite decades of innovation in cybersecurity, traditional defenses continue to fall short against modern malware. Attackers have learned to exploit the weaknesses of systems built for a different era. The result is a widening gap between how quickly malware adapts and how slowly conventional defenses respond.

Legacy Secure Email Gateways Often Miss Attacks With No Static Indicators

Secure email gateways (SEGs) were designed to detect known threats, matching inbound content against blocklists, reputation databases, and malware signatures. While effective against high-volume spam or commodity phishing, these tools struggle to detect advanced attacks that lack traditional indicators.

Modern malware frequently arrives without obvious red flags: no malicious attachments, no suspicious links, and no detectable code prior to execution. Instead, it leverages social engineering and context manipulation—impersonating trusted contacts, using legitimate collaboration platforms, or embedding content that only becomes harmful after delivery. Because SEGs depend on static threat data, they cannot consistently recognize these dynamic, intent-driven attacks.

As a result, sophisticated malware routinely bypasses detection, reaching users who perceive it as safe.

Sandbox Evasion Through Encryption and Password Protection

Many organizations supplement SEGs with sandboxing technologies that analyze attachments or URLs in isolated environments. However, adversaries have grown adept at evading these measures.

Unfortunately, encrypted or password-protected files prevent sandbox tools from scanning their contents altogether, and time-delayed payloads can remain dormant until well after analysis concludes. In some cases, malware even detects when it is running in a virtual environment and alters its behavior to appear benign.

These evasion techniques make it increasingly difficult for traditional inspection-based tools to distinguish legitimate content from malicious intent, leaving organizations with a false sense of security.

The Human Reporting Gap

Even with layers of technology, many organizations still rely on employees to identify and report suspicious messages. This gap is not due to negligence—it reflects the sophistication of modern social engineering. Messages are crafted to appear authentic, often tailored to individual recipients or business processes. Employees rarely have the context needed to identify subtle anomalies in tone, timing, or sender behavior.

Furthermore, the reliance on manual reporting creates a latency problem. By the time a user flags a suspicious message, the attacker may already have achieved their objective—compromising credentials, executing code, or exfiltrating data. The combination of human fallibility and delayed response allows many advanced threats to succeed where technology alone cannot.

An Asymmetric Advantage for Attackers

Together, these cracks in cybersecurity armor give adversaries a significant advantage. To keep pace, organizations must shift from reactive detection to proactive understanding—moving beyond static indicators toward behavioral and contextual awareness that reflects how modern attacks actually unfold.

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Anatomy of Modern Attacks

Modern malware doesn't announce itself with flashing alerts or corrupted files. It hides behind familiar names, trusted brands, and believable requests —using credibility and context to trick users into opening the door for them.

A typical malware campaign follows a clear chain of events:

Step 1: The Lure

The attack begins with a phishing email designed to look legitimate, often impersonating a known vendor, a government agency, or an internal department. It references something routine, like an HR document, a tax form, or a policy update, and urges immediate review. The message looks authentic enough to bypass suspicion and reach the inbox.

Step 2: The Delivery

Instead of attaching an obvious executable, the attacker links to a cloud-hosted, encrypted, or password-protected file. The file appears safe—hosted on a trusted service and labeled professionally—but once downloaded, it contains the malware. Because it uses legitimate infrastructure, it easily evades filters that rely on static indicators or domain reputation.

Step 3: The Execution

When the user opens the file, the malware quietly installs. Sometimes it's a traditional payload, other times as fileless code that runs directly in memory. Either way, it establishes persistence, connects to a remote command-and-control server, and gives the attacker access to the system.

Step 4: The Spread

With access established, the attacker moves laterally through the environment. They steal credentials, search for shared drives, and target high-value accounts or systems. Each step expands control and prepares the ground for larger payloads, including ransomware.

Step 5: The Payoff

Once they have what they need, the attacker launches the final phase—data theft, encryption, or extortion. Files are locked, sensitive data is exfiltrated, and the victim receives a ransom note demanding payment to restore access or prevent disclosure.

These malware campaigns succeed because they don't look malicious. No suspicious domains. No corrupted attachments. No detectable signatures. They exploit trust, timing, and human behavior—not system flaws. And because traditional tools can't see intent, these attacks often unfold unseen until it's too late.

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Defensive Strategies for CISOs

As the frequency and sophistication of malware and ransomware continue to rise, CISOs face mounting pressure to adapt. The traditional perimeter no longer exists. Effective defense now requires a modern, integrated framework, one that leverages automation, behavioral analytics, and continuous visibility across email, cloud applications, and endpoints.

Behavioral AI For Email and Applications

Modern attacks rarely present clear technical indicators. Instead, they exploit behavioral signals: unusual timing, tone shifts, or context deviations. Behavioral AI helps close this gap by learning what “normal” communication and activity look like within an organization. By establishing baselines for users and systems, deviations become instantly visible, allowing for rapid detection of impersonation attempts, credential abuse, or hidden malware delivery.

Continuous Monitoring and Automation

API-based integrations have transformed the speed of detection and response. Unlike legacy tools that poll data or rely on gateway filtering, API-driven systems analyze messages and user actions in real time, identifying threats and remediating them in seconds without disrupting mail flow or productivity. Automated response actions, such as quarantining messages or disabling compromised accounts, dramatically reduce mean time to detect (MTTD) and mean time to respond (MTTR).

Threat Intelligence Sharing

No organization operates in isolation. Modern defensive strategies rely on collective insight, aggregating telemetry across industries and regions to identify new malware strains and evolving ransomware variants. Shared intelligence helps defenders recognize patterns early, reducing the dwell time of active threats and improving the accuracy of prevention models.

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

Conclusion

The speed of ransomware and malware innovation now exceeds the capacity of many organizations to defend against them. Human error, email-based delivery, and the growth of ransomware-as-a-service have created an environment where even well-funded organizations are at risk.

For CISOs, the path forward lies in adopting behavioral intelligence, automation, and adaptive security operations to build measurable resilience. By combining real-time behavioral analytics with continuous monitoring, shared intelligence, and integrated response workflows, security leaders can close the gap between unseen risks and actionable defense.

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED

About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 20% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Prevent Attacks Targeting Human Behavior Today

See a Demo ›

Discover Your ROI ›

© 2025 ABNORMAL AI, INC. // ALL RIGHTS RESERVED